Networking Fundamentals #2 Homework

Mission 1.

Determine and document the mail servers for starwars.com using NSLOOKUP.

```
Server:         8.8.8.8
Address:    8.8.8.8#53

Non-authoritative answer:
starwars.com    mail exchanger = 10 aspmx2.googlemail.com.
starwars.com    mail exchanger = 5 alt1.aspx.l.google.com.
starwars.com    mail exchanger = 1 aspmx.l.google.com.
starwars.com    mail exchanger = 10 aspmx3.googlemail.com.
starwars.com    mail exchanger = 5 alt2.aspmx.l.google.com.

Authoritative answers can be found from:
```

Explain why the resistance isn’t receiving any emails.

After running the nslookup -type=MX starwars.com command it’s apparent they are not receiving emails because the server is different from the servers they have assigned to starwars.com. The emails cannot find the destination because of this.

Document what corrected DNS record should be.

The DNS should be reconfigured to allow asltx.l.google.com to be the primary server with a value of 1. The secondary default server at asltx.2.google.com should be set to 5 in case server 1 fails it can reroute.

Mission 2

Determine and document the SPF for theforce.net using NSLOOKUP.

```
starwars.com       text =
"google-site-verification=3qYuZ0m5YJdjmVslnraXZKQtXmO_3YI9wv6nCY1CPHM"
starwars.com       text =
"google-site-verification=GohBbB11BuN1VTA3oFWu3tmiM_pM4Bw_nzKAonQmDb8"
starwars.com       text = "v=spf1 include:mail.zendesk.com ?all"
```

<u>Explain why the Force's emails are going to spam.</u>

After running the nslookup -type=TXT starwars.com command you see that the SPF file cannot verify the emails so it sends them to the spam folder.

<u>Document what a corrected DNS record should be.</u>

The correct DNS would be altered to allow the IP address of 45.23.176.21 to be added to the authorized IP addresses so that it can verify and then receive them in the primary inbox and not the spam folder.

Mission 3.
Issue: You have successfully resolved all email issues and the resistance can now receive alert bulletins. However, the Resistance is unable to easily read the details of alert bulletins online.

<u>Document how a CNAME should look by viewing the CNAME of www.theforce.net using NSLOOKUP.</u>

After running the nslookup -type=CNAME theforce.net command this was the output:

```
Server:            8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
*** Can't find theforce.net: No answer

Authoritative answers can be found from:
```

```
theforce.net
        origin = WebPublish_Othe
        mail addr = hostmaster
        serial = 2017110901
        refresh = 900
        retry = 600
        expire = 86400
        minimum = 3600
```

The results of nslookup -type=CNAME resistance.theforce.net:

```
Server:         8.8.8.8
Address:    8.8.8.8#53

** server can't find resistance.theforce.net: NXDOMAIN
```

<u>Explain why the sub page of resistance.theforce.net isn't redirecting to theforce.net</u>

The sub page is not redirecting because there is no domain to redirect from.

<u>Document what a corrected DNS record should be.</u>

The domain would need to be assigned to resistance.theforce.net in order for the redirection to take place.

Mission 4:

Issue: During the attack, it was determined that the Empire also took down the primary DNS server of princessleia.site.

<u>Confirm the DNS records for princessleia.site.</u>

After running the command: nslookup -type=SRV princessleia.net the results were:

```
Server:         8.8.8.8
Address:    8.8.8.8#53
```

```
Non-authoritative answer:
*** Can't find princessleia.net: No answer

Authoritative answers can be found from:
princessleia.net
        origin = ns1.dnsowl.com
        mail addr = hostmaster.dnsowl.com
        serial = 1637223364
        refresh = 7200
        retry = 1800
        expire = 1209600
        minimum = 600
```

As well as the command: nslookup -type=A princessleia.net

The results are:

```
Server:         8.8.8.8
Address:    8.8.8.8#53

Non-authoritative answer:
Name:       princessleia.net
Address: 107.161.23.204
Name:       princessleia.net
Address: 192.161.187.200
Name:       princessleia.net
Address: 209.141.38.71
```

Document how you would fix the DNS record to prevent this issue from happening again.

In order to prevent the issue of problems from happening in the future the the primary server should have the backup server of ns2.galaxybackup.com added to the zone file or cache.

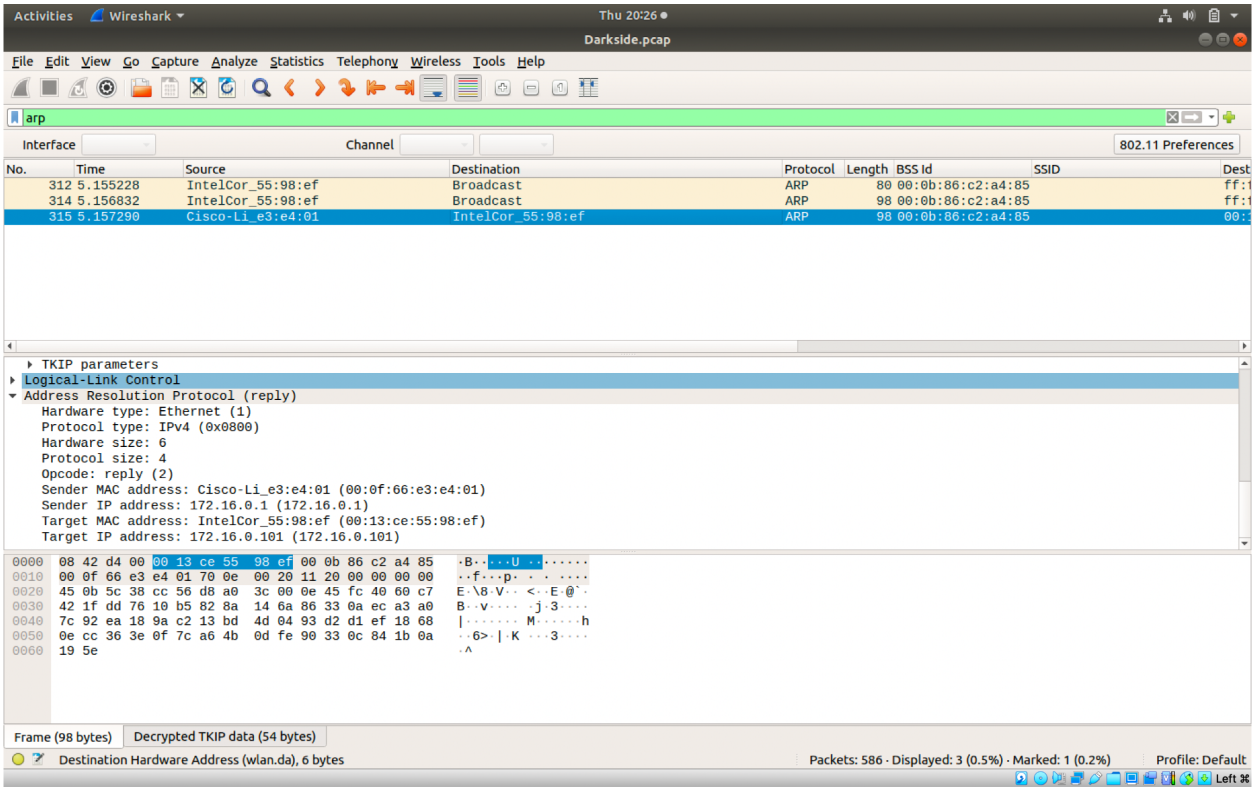
Mission 5:

Confirm your path doesn't include Planet N in its route.

The shortest path from Batuu to Jedha is:
D,C,E,F,J,K,O,R,V

Mission 6:

Document these IP and MAC Addresses, as the resistance will use these IP addresses to launch a retaliatory attack.



arp

```
No.   Time      Source              Destination         Protocol Length BSS Id             SSID  Dest
  312 5.155228  IntelCor_55:98:ef   Broadcast           ARP          80 00:0b:86:c2:a4:85        ff:1
  314 5.156832  IntelCor_55:98:ef   Broadcast           ARP          98 00:0b:86:c2:a4:85        ff:1
  315 5.157290  Cisco-Li_e3:e4:01   IntelCor_55:98:ef   ARP          98 00:0b:86:c2:a4:85        00:1
```

```
  ▸ TKIP parameters
▸ Logical-Link Control
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Cisco-Li_e3:e4:01 (00:0f:66:e3:e4:01)
    Sender IP address: 172.16.0.1 (172.16.0.1)
    Target MAC address: IntelCor_55:98:ef (00:13:ce:55:98:ef)
    Target IP address: 172.16.0.101 (172.16.0.101)
```

```
0000  08 42 d4 00 00 13 ce 55  98 ef 00 0b 86 c2 a4 85   ·B······U ········
0010  00 0f 66 e3 e4 01 70 0e  00 20 11 20 00 00 00 00   ··f···p· · · ····
0020  45 0b 5c 38 cc 56 d8 a0  3c 00 0e 45 fc 40 60 c7   E·\8·V·· <··E·@`·
0030  42 1f dd 76 10 b5 82 8a  14 6a 86 33 0a ec a3 a0   B··v···· ·j·3····
0040  7c 92 ea 18 9a c2 13 bd  4d 04 93 d2 d1 ef 18 68   |······· M······h
0050  0e cc 36 3e 0f 7c a6 4b  0d fe 90 33 0c 84 1b 0a   ··6>·|·K ···3····
0060  19 5e                                              ·^
```

Frame (98 bytes) | Decrypted TKIP data (54 bytes)

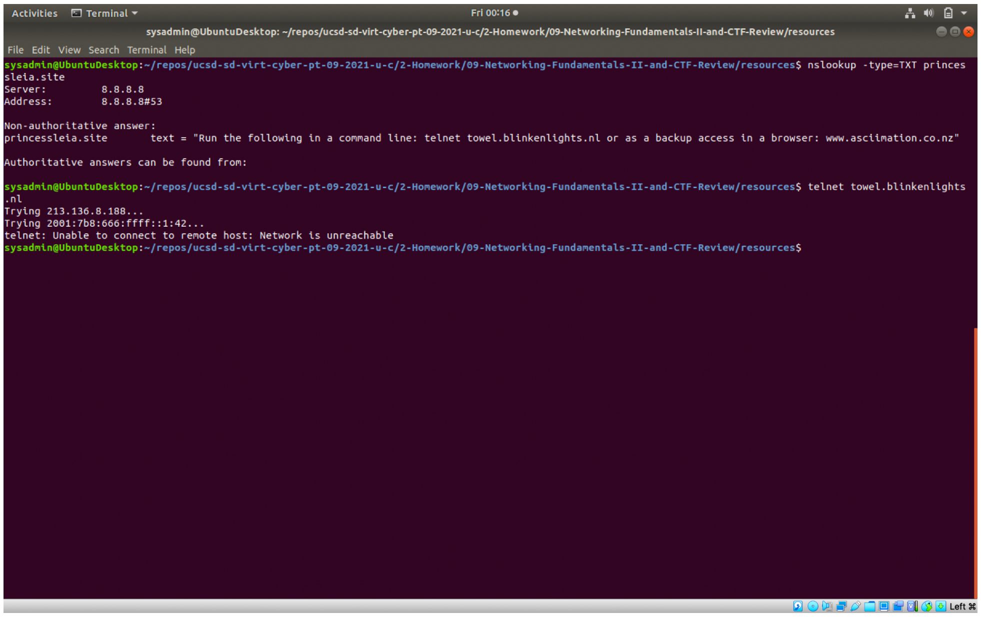
Destination Hardware Address (wlan.da), 6 bytes   Packets: 586 · Displayed: 3 (0.5%) · Marked: 1 (0.2%)   Profile: Default

The IP addresses are as follows:
Sender:
IP address- 172.16.0.101
MAC address- 00:0f:66:e3:e4:01

Target:
IP address- 172.16.0.1

MAC address- 00:13:ce:55:98:ef

Mission 7:


Activities
Terminal
Fri 00:16
sysadmin@UbuntuDesktop: ~/repos/ucsd-sd-virt-cyber-pt-09-2021-u-c/2-Homework/09-Networking-Fundamentals-II-and-CTF-Review/resources
File Edit View Search Terminal Help

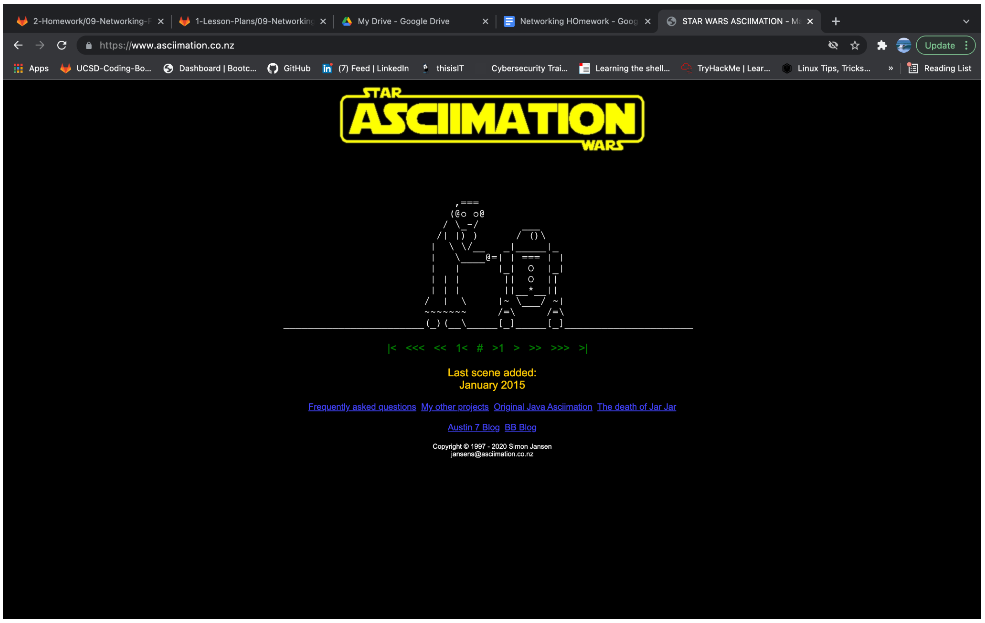
```
sysadmin@UbuntuDesktop:~/repos/ucsd-sd-virt-cyber-pt-09-2021-u-c/2-Homework/09-Networking-Fundamentals-II-and-CTF-Review/resources$ nslookup -type=TXT princes
sleia.site
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
princessleia.site       text = "Run the following in a command line: telnet towel.blinkenlights.nl or as a backup access in a browser: www.asciimation.co.nz"

Authoritative answers can be found from:

sysadmin@UbuntuDesktop:~/repos/ucsd-sd-virt-cyber-pt-09-2021-u-c/2-Homework/09-Networking-Fundamentals-II-and-CTF-Review/resources$ telnet towel.blinkenlights
.nl
Trying 213.136.8.188...
Trying 2001:7b8:666:ffff::1:42...
telnet: Unable to connect to remote host: Network is unreachable
sysadmin@UbuntuDesktop:~/repos/ucsd-sd-virt-cyber-pt-09-2021-u-c/2-Homework/09-Networking-Fundamentals-II-and-CTF-Review/resources$
```

The instructions for the first command did not work so I used the web browser address to access my reward! The force is with me!



Last scene added:
January 2015

Frequently asked questions My other projects Original Java Asciimation The death of Jar Jar

Austin 7 Blog BB Blog

Copyright © 1997 - 2020 Simon Jansen
jansens@asciimation.co.nz